Battlespace Systems Support Directorate Bulletin

January 2004
Volume 2, Issue 2

"Serving the Needs of the Battlespace Systems Community"

Inside this Issue

*The **BSSD Bulletin** is published quarterly under supervision of the Director, US Army Communications Electronic Command (CECOM) Software Engineering Center (SEC), Battlespace Systems Support Directorate to provide DoD, military, and civilian personnel information on technical development, issues, and ideas of and about the Directorate. The views and opinions expressed are not necessarily those of the Department of the Army, CECOM, or the SEC.*

Brigade Subscriber Node & Network Operations Center-Vehicle: An Integral Part of the Stryker Brigade Combat Team

Submitted by Yat Chan, Brian Coombs, and Ekta Parikh, CECOM SEC

The Stryker Brigade Combat Team (SBCT) is a ***full spectrum, combat force***. It has utility, confirmed through extensive analysis, in all operational environments against all projected future threats, but it is designed and optimized primarily for employment in small-scale contingencies in complex and urban terrain, confronting low-end and mid-range threats that may employ both conventional and asymmetric capabilities. The SBCT deploys very rapidly, executes early entry, and conducts effective combat operations immediately on arrival to prevent, contain, stabilize, or resolve a conflict through shaping and decisive operations. The SBCT participates in major theater war, with augmentation, as a subordinate maneuver component within a division or corps, in a variety of possible roles. The SBCT also participates with appropriate augmentation in stability and support operations as an initial entry force and or as a guarantor to provide security for stability forces by means of its extensive combat capabilities. Brigade Subscriber Node (BSN) and Network Operations Center-Vehicle (NOC-V) support the SBCT by providing state-of-the-art communications capabilities. The BSN combines voice, data, and video switching with organic transmission capabilities in order to provide a smaller, lighter, more capable system than today's Army Common User System can achieve. The BSN and NOC-V provide both secure and non-secure communications for the Warfighter, as well as communications management capabilities, in order to increase situational awareness.

Continued on page 4

"Advanced Heads Up Display" Product Manager Gets Demo Capability

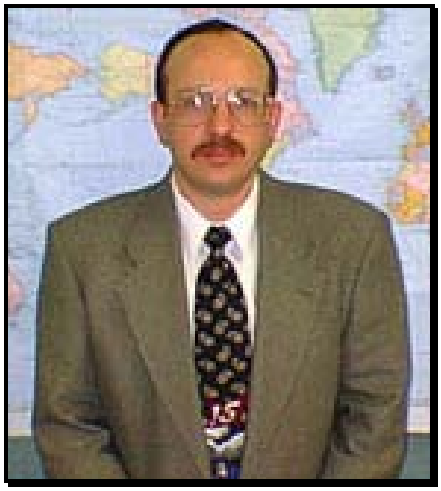
Submitted by Kwok Lo, CECOM SEC

Under a joint venture with the Advanced Heads Up Display (AHUD) Program Office, the CECOM SEC has developed a Portable Demonstration Unit to showcase the capabilities of the AHUD. Everyone wants the Warfighter to have access to the best technology to safely and effectively complete his mission. However, it is difficult sometimes to justify the cost of systems when they cannot be demonstrated to the decision makers. The SEC understands this need, and, with the creation of the Portable Demo Unit, has effectively solved this problem for the AHUD product manager.

Continued on page 3

From the Senior Editor's Desk
Attitude and the Group Dynamic

Commentary By Joseph Ingrao, Deputy Director, Battlespace Systems Support



"Great harm has been done to us. We have suffered great loss. And in our grief and anger we have found our mission and our moment. Freedom and fear are at war. The advance of human freedom—the great achievement of our time, and the great hope of every time—now depends on us. Our nation—this generation—will lift a dark threat of violence from our people and our future. We will rally the world to this cause by our efforts, by our courage. We will not tire, we will not falter, and we will not fail."

President George W. Bush at the Joint Session of Congress, September 20, 2001

As a manager and a leader, nurturing a positive attitude in your employees is of paramount importance—this is especially true in the group dynamic. Group participation involves a joint effort between the group and the group leader in arriving at decisions in such a way that everyone can sense that others are considering their ideas. An important advantage of the group dynamic is that more creative decisions will emerge. This creativity will occur only if the attitude of the group is such that it allows a permissive atmosphere in which all group members freely express their thoughts. A group can almost always generate better decisions than the 'go it alone' approach. For example, in bicycle racing, the peleton (group) is faster than the lone rider.

Creating a positive work environment is not easy. First, and of paramount importance, you the manager must exhibit a positive attitude. You often set the tone for the work environment. Focus on what you can control: making work interesting, offering praise and recognition, involving employees in the decision making process, and the like. We must not lose site of the fact that attitude is an important management tool.

Fostering positive attitudes along with encouraging group participation should be goals of all managers.

"Advanced Heads Up Display" Product Manager Gets Demo Capability
(Continued from page 1)

The AHUD products were developed to allow a pilot to monitor critical helicopter flight data control information, without taking his eyes "off the road." The products assist a pilot in monitoring the changing terrain and flight control data in order to ensure a safe and successful flight mission. Helicopter and flight information is gathered and converted into an easy to understand pictograph by a Signal Data Converter (SDC). This pictographic display is presented as an unobtrusive line drawing in the pilot's night vision goggles by the Display Unit. The pilot is able to monitor important flight parameters such as altitude, speed, pitch, and heading direction, as well as aircraft faults, such as engine fires, without taking his eyes off of the terrain.

Until recently, the only way the capabilities of the AHUD system could be seen, short of being a helicopter pilot, was to bring along the Aircraft Training Simulator (ATS). The ATS, measuring 2 ft × 3 ft × 3 ft and weighing 385 lbs, was never practical for demonstrating the AHUD products. The SEC found a solution to this dilemma by developing a Portable Demo Unit. Using a MIL-STD 1553 data bus, all the functionality of an AHUD display can be demonstrated in a portable fashion, enabling a wider audience to experience this technology. The Portable Demo Unit allows pilots and decision makers to view exactly how the display indicates important flight parameters. The demo has an auto run script, which dynamically depicts how the graphics change during an actual flight.

A Visual Basic program that runs on a PC controls the Portable Demo Unit. With its intuitive user interface, a demonstrator of the AHUD is able to modify any parameter sent to the SDC with ease, as all the parameters are clearly labeled. As the controls are altered, the PC assembles a data packet containing the simulated flight parameters and sends it to the SDC. The program within the SDC has been modified to accept these data from the 1553 bus instead of checking its analog, or synchro inputs to extract the data. The symbol generation routines within the SDC are unaware of the source of the data, and operate in their usual fashion. The Portable Demo Unit has a display unit and a camera contained within its enclosure, which enables a large copy of the AHUD display to be shown to an audience.

The AHUD Portable Demo Unit allows the AHUD product line to be brought to a conference or meeting with ease. All the components needed to set up and showcase the AHUD system easily fit in a single carrying case, and, just as important to the demonstrator, this system can be set up and broken down in a matter of minutes. The Portable AHUD Demo system is an achievement in convenience and technology, as well as making it possible for those in the industry to be aware of the advancements in helicopter flight safety. When the SEC demonstrated the Portable Demo Unit at an AUG 03 meeting to PM Mark Salverson, he raved about how important this technology would be to him. Mr. Salverson said "I need to put the AHUD helmet on congressmen, generals, and other decision makers!" As a result of this effort, the PM Office has provided additional funding to SEC to build several AHUD Portable Demo Units. ■

Brigade Subscriber Node & Network Operations Center-Vehicle:
An Integral Part of the Stryker Brigade Combat Team

(Continued from page 1)

The BSN system comprises commercial and government-owned communications hardware and software to provide voice, video, and data transmissions. The BSN has routers for data, a PBX (Private Branch Exchange) for voice call switching, TACLANE and KIV-19 for encryption, an operators' workstation to control and monitor the communication systems, a Network Planning Terminal (NPT), and a Mobile Subscriber Equipment (MSE)/Tri-Services Tactical switch interface device, Vantage, that provides flood search routing and Tactical User Identifications.

Network management is an integral part of the BSN system. BSN has the ability to plan, engineer, monitor, and manage the BSN switch network. BSN hosts network management client-servers with commercial and government-developed tools which manage the BSN nodal and Wide Area Network (WAN)/Local Area Networks (LAN). BSN also hosts the sensitive but unclassified network management functionality while providing Information Assurance (IA) planning and managing for the SBCT network. Besides network management, BSN also integrates High Capacity Line of Sight (HCLOS) terrestrial radios for dual homing transmission links. BSN can provide three simultaneous satellite links using an organic transmission stack common to NOC-V, Digital Bridge, and Single Shelter Switch BBN.

The NOC-V provides the S6 with an integrated network capability for managing, supporting, planning, and monitoring the Tactical Operations Center (TOC) LAN and the Lower Tactical Internet (TI). The NOC-V consists of Army radios (EPLRS, SINCGARS, and an NTDR), network operations hardware (router, switches, and a server), commercial network management software (HP Openview, and Cisco Works 2000), and various Government Furnished Equipment (GFE). The GFE includes Force XXI Battle Command Brigade and Below (FBCB2) suite, Tactical Internet Management System, NPT, Maneuver Control System-Lite, along with the Global Broadcasting System (GBS), Wireless LAN, and TOC Intercom. The NOC-V configuration is designed with components to support future technical insertion to provide improved network operations capabilities to the SBCT.

The NOC-V plans, engineers, monitors, and manages the TOC LAN within its management domain. It manages users within the TI and provides the capability to exchange information with organizations and individuals that are not directly connected to the TOC LAN. While the NOC-V does not have a WAN requirement, it can monitor the WAN for mission critical network awareness. NOC-V provides protection and defense of data networks and information systems through aggressive application of IA measures (i.e., virus scanning). By implementing IA procedures, the NOC-V uses security measures to ensure network availability, integrity, authentication, and confidentiality within its managed LAN.

NOC-V has a requirement to pass data traffic to MSE, the Small and Large Extension Nodes, and to the Node Center Switch. NOC-V interfaces with the BSN to send traffic to the MSE Network. NOC-V can connect to an external network outside the TOC either through the BSN connection or directly through a SMART-T connection (see figure on page 5).

NOC-V and BSN are managed by Program Manager Tactical Radio Communications Systems (PM-TRCS). Both systems are developed by CECOM RDEC Space and Terrestrial Communications Directorate (S&TCD). BSN version 1 (SBCT1 and SBCT2) has previously transitioned to SEC for Post Production Software Support (PPSS). SEC provides PPSS software updates to the field, and works closely with S&TCD on PPSS transition for BSN version 2, a new version that integrates additional requirements. SEC is an active participant in the NOC-V effort, providing software oversight for PM-TRCS, and preparing for Post Deployment Software Support, which will begin in FY05. SEC has become familiar with the NOC-V and BSN configurations and software by becoming integrated within the S&TCD team; this was accomplished by attending weekly status meetings, assisting in troubleshooting problems, participating in test events, and providing support to the S&TCD team.

In order to prepare for the transfer of BSN to SEC, all procedures were verified to ensure that the equipment, once installed, would execute the BSN operational software and function with the target software. S&TCD provided SEC with all of the necessary software and hardware procedures to carry out these verification tasks. After transitioning to SEC, S&TCD personnel have continued to provide post transition assistance. Additionally, S&TCD has provided instructions on the integration of COTS (commercial off-the-shelf) components into the BSN system, operational instruction on the BSN, and on-the-job training. SEC and S&TCD jointly managed the transition of the BSN SBCT1 and SBCT2 software baseline. SEC ensures that any changes are controlled and coordinated with other functional areas and organizations. S&TCD is responsible for developing retrofits to future BSN versions while SEC performs PPSS on those versions that have been fielded to operational units. SEC and S&TCD work closely on all efforts and have successfully established an Integrated Product Team.

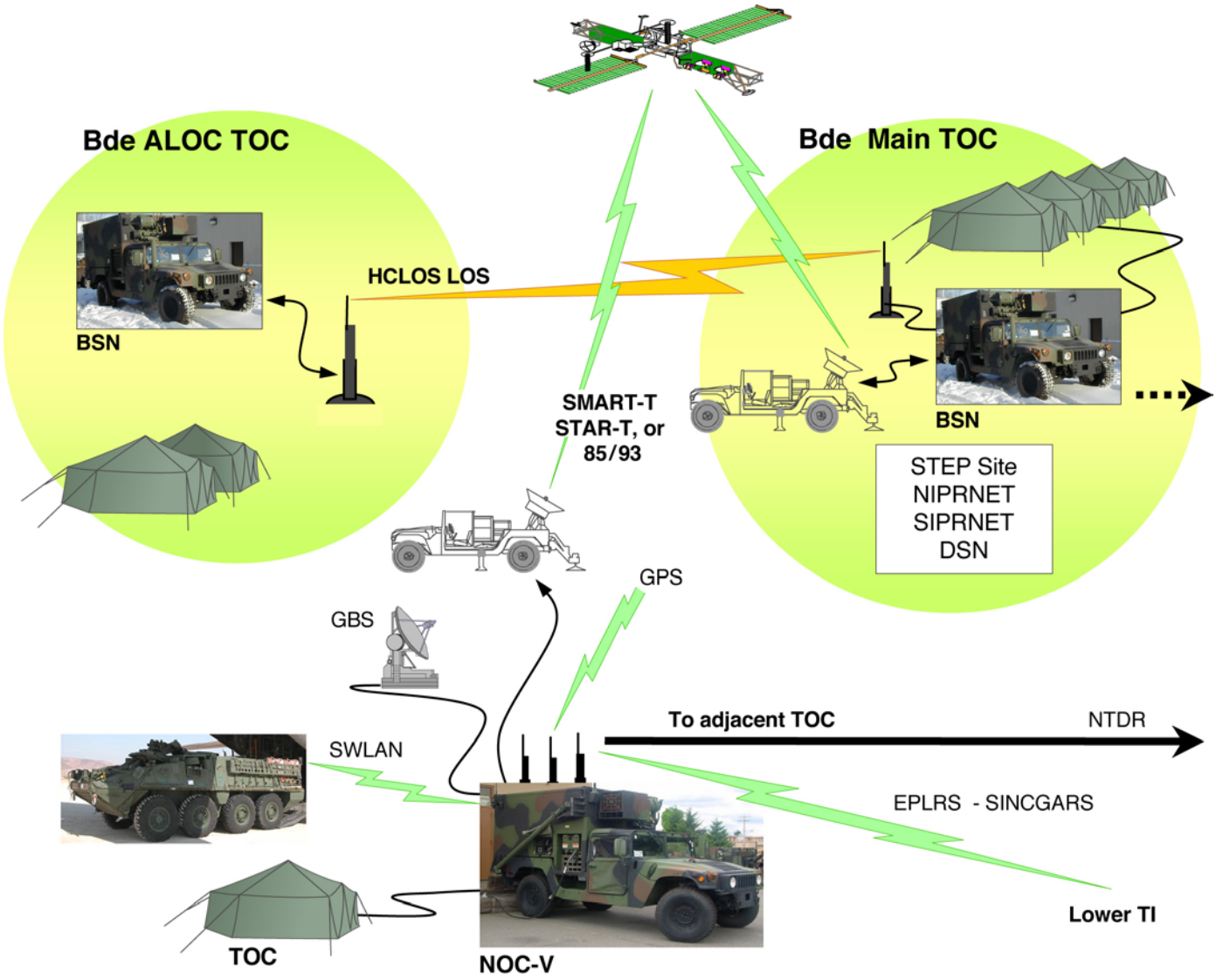
Continued on page 5

Brigade Subscriber Node & Network Operations Center-Vehicle:
An Integral Part of the Stryker Brigade Combat Team

(Continued from page 4)

Several steps are being taken in order to ensure a smooth transition of the NOC-V software from S&TCD to SEC, which is scheduled to take place in FY05. SEC developed the appropriate documentation for establishing a Configuration Control Board, provided comments on S&TCD-generated documents, and assisted in generating a project schedule. In addition, SEC also provided the capability of tracking Field Incident Reports (FIRs) via the SEC FIR website and developed a stand-alone version of the same tracking database for use where Internet access is unavailable.

The development of SBCT 1–3 NOC-V systems is close to completion and will be transitioned to SEC after NOC-V undergoes a Limited User Test, currently scheduled for late FY04. SBCT 4 vehicles will be developed once the SBCT 3 development is completed. SBCT 4 vehicles and configuration will transition to SEC at a later date. ■



SINCGARS—Evolving to Meet the Challenges of the 21st Century

Submitted by Hamed Yousef, CECOM SEC

SINCGARS ASIP RT-1523E Radio

Single Channel Ground and Airborne Radio System (SINCGARS) is the primary Combat Net Radio for the US Army. It is designed for processing voice, analog, and digital data to provide commanders with a highly reliable, secure, and easily maintainable system in support of command and control operations. SINCGARS, a very high frequency, frequency modulated radio system, operates on all 2320 frequency channels between 30 and 88 MHz and employs frequency hopping as its primary means for electronic counter countermeasure of communications against a hostile (jamming) environment. SINCGARS is designed modularly to achieve maximum commonality among the various ground and airborne system configurations.

The first SINCGARS radio produced was the RT-1439. This radio required an external KY-57 VINSON Communications Security (COMSEC) to encrypt and de-encrypt messages. The Army received approval from the National Security Agency to embed COMSEC within the SINCGARS radio to reduce the load of the MANPACK user and at the same time reduce the amount of external crypto devices required for the Army. This resulted in the subsequent release of the RT-1523, and was termed the SINCGARS Integrated COMSEC (ICOM) radio. In order to meet the demands of fielding, the Department of the Army authorized a second source to produce SINCGARS ICOM radios that are Form, Fit, and Function interchangeable at the Line Replaceable Unit level. The second source introduced significant product improvements to include Cosite performance, improved battery life, and enhanced low-speed operation. These enhancements were incorporated back into the initial source product line and resulted in the production of the RT-1523A and RT-1523B ICOM radios.

In line with the Army's move toward digitization, users have expressed the need to increase their communications functionality and capability, which led to the development of the SINCGARS System Improvement Program (SIP). The SIP radio (RT-1523C and RT-1523D) incorporated features such as an interface to an external Precision Lightweight Global Position System Receiver, improved Forward Error Correction, and Packet routing. These improvements along with the introduction of the Internet Controller (INC) card, provided the mechanics for Internet Protocol routing between radio nets and other communications systems (Enhanced Position Location and Reporting System, Local Area Networks, etc.), which revolutionized the way data are transmitted across the battlefield.

SINCGARS participated in the Army's Task Force XXI Advanced War-Fighting Exercises in which the use of Tactical Internet and Packet data was deployed for the very first time. Although this proved that the concept of the Tactical Internet was achievable, there were many factors that affected the performance of the communication system. Among them were the effects of Cosite, net surfing, voice and data contention, and the amount and frequency of data being placed on the net. To address these deficiencies, the Advanced SIP (ASIP) radio was introduced, which incorporated an Enhanced SIP waveform, which included optimization to algorithms of the Noisy Channel Avoidance scheme, the Time of Day tracking scheme, and the End of Message scheme. The ASIP radio will provide improved data capability, improved forward error correction for low speed data modes, a GPS interface, and an INC, which allows SINCGARS to interface with EPLRS and Battlefield Functional Area host computers.

Continued on page 7

SINCGARS—Evolving to Meet the Challenges of the 21st Century

(Continued from page 6)

The ASIP radio (RT-1523E) is a repackaged RT-1523C SIP radio, and physically is one-half the width and one-third the weight of a full size radio. Recent improvements to the INC include a more powerful microprocessor with increased memory. The ASIP configuration is targeted toward the dismounted soldier and will complete the SINCGARS production.

The primary mission of SINCGARS is to provide highly reliable secure voice communications. As user data communication needs grow, it will be necessary to increase the SINCGARS data capacity while maintaining reliable secure voice services. By combining advanced voice compression technology, data can be transmitted simultaneously with voice on a noninterfering basis. This new capability is termed Simultaneous Independent Voice and Data.

Unlike other major weapon systems where carbon copies of the same product are produced over and over again, the SINCGARS radio program has continuously evolved to provide the latest in improvements and capabilities to the Warfighter and strive to meet the Army's objectives for digitization. ■

The Evolutionary Acquisition of the Future Combat Systems

Submitted by Akbar Khan, CECOM SEC

Evolutionary acquisition of software systems in even the most favorable of circumstances is an extremely challenging undertaking, where acquisition professionals are forced to use their years of training and experience to resolve problems that are not completely defined. But when the Army orders the procurement of a revolutionary new system—called the Future Combat Systems (FCS)—that will literally transform the way the Army does business, these same Government employees can no longer rely on the standard acquisition tools and practices to meet programmatic requirements. Instead, these personnel must stretch their imaginations and develop completely new means to translate idealistic operational objectives into a viable and functional system. This involves orchestrating a spiral software development with a wide range of suppliers and contractors to build a state-of-the-art system with evolving requirements and insertion of futuristic technologies. All during the process, the Government Team will serve in the following capacities to ensure project success:

- **Communications Link** between the user and contractors—to channel vital information to where it is needed
- **Quality Assurance Team**—to make certain that technical standards are being met
- **Management Watchdog**—to monitor scheduling and programmatic progress
- **Fire Rescue Team**—to resolve unexpected problems
- **Program Champion**—to obtain required funding and political support

The challenge is to function in all of these roles in a seamless and consistent manner to keep the acquisition program on track.

The ideas outlined above are not merely theoretical visions of an academician, but instead are based on my actual experience serving as a member of the Government Management Team charged with overseeing the development of Future Combat Systems command and control software. The FCS Software Development Plan describes the system as follows:

> Future Combat Systems is a family of advanced, networked air and ground-based maneuver, maneuver support, and sustainment systems that will include manned and unmanned platforms. The FCS systems are networked together via a distributed system architecture that includes networked communications, network operations, sensors, battle command systems, and manned and unmanned reconnaissance and surveillance capabilities to enable levels of situational understanding and synchronized operations heretofore unachievable.

In simple terms, the myriad of modules that provided individual functionalities already existed, but what was unprecedented was the integration of all these capabilities into one system. Thus, it was decided to develop customized middleware to serve as an interconnection among the software services that would make up the FCS software family. Compounding the formidable technical challenges in developing such unprecedented software was the extremely aggressive schedule set by the Army. To have any chance of meeting this Army mandate, it was decided to pursue a series of successive software builds with requirements development, software design, and implementation occurring in concurrent fashion.

Continued on page 8

(Continued from page 7)

Organizationally, the Government and the Lead Systems Integrator combined resources into one Integrated Product Team to navigate through the choppy waters of software development and operated in an almost seamless manner with technical and programmatic responsibilities being assumed on a mutual basis. To date, this joint approach has yielded a robust start to the software development effort and allowed both sides to contribute as best as they can to the overall effort without relinquishing their formally defined roles. In conclusion, it can be seen that innovation and team spirit have both contributed to the overall success of the FCS software build effort. ■

SEC IFS Develops Software Problem Report Portalization

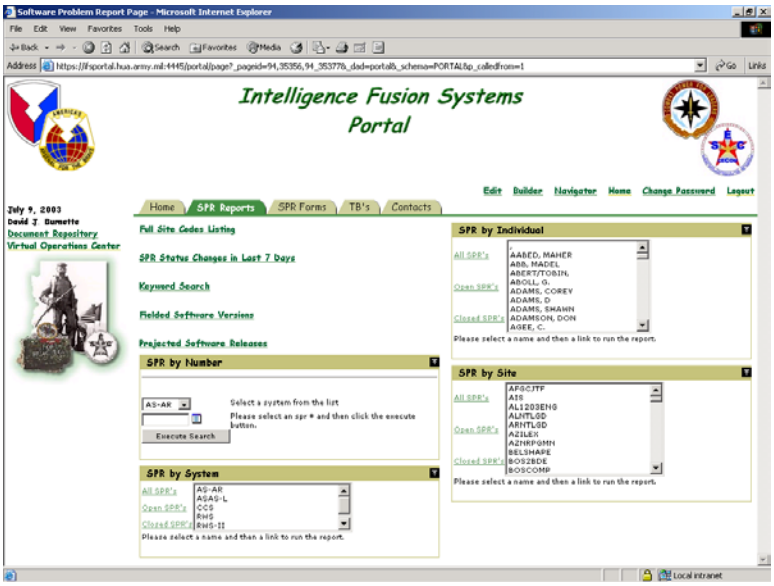
Submitted by Hal Clause, CECOM SEC

US Army CECOM SEC, Intelligence Fusion Systems (IFS) Division is in the development phase of establishing an Enterprise Portal for the Software Problem Report (SPR) process to support global management of Software Engineering and Field Software Engineering SPR activities. The portal is an online business intelligence system providing an information management gateway to users from different communities. The portal will connect the different communities together through an extensible framework via a web interface. The high maintenance of "thick" client-server technology will be replaced with a network-centric and centralized repository accessible through a web browser over a secure connection using Secure Socket Layer (SSL) communications. The SPR process will be visible from problem to solution.

The portal is part of the Oracle 9i Application Server (Oracle9iAS) product line. It is fully compliant with Internet application building standards. It supports technologies such as Java 2 Enterprise Edition, Web Services, Lightweight Directory Access Protocol (LDAP), SSL, and several Extensible Markup Language standards. Oracle-9iAS has high availability features that include fault tolerance, clustering, online maintenance, and integrated security management to satisfy mission critical requirements. Because it employs industry standard technologies, rapid development using an existing development staff can be achieved at a lower cost. The portal will be able to integrate applications built in Oracle9iAS with existing systems and business partners to provide data consolidation. Since the portal is an Internet application, it will allow desktop application consolidation. Through LDAP, the portal will achieve a true single sign-on feature by allowing users signed on to the Army Knowledge Online (AKO) site to be signed automatically on to the portal site. The scalability of the portal will offer a service around which other services can be built.

Report generation of information in the SPR database will be customizable and publishable. Ad hoc reports as well as standard reports will be available. The power of ad hoc reports will give the user access to all available information in an individually tailored format for easier review and analysis. Any report can then be saved for repeated use or published to the user community and become part of the standard report pool.

Creating an Enterprise Portal to the SPR database will modernize the life cycle support of fielded systems. It will decrease Total Cost of Ownership by providing a web interface to a central data repository in place of the high maintenance "thick" client-server interface. It will allow secure, global accessibility through an SSL enabled web browser. It will increase productivity by offering a Help Desk system linked to a knowledge center and eliminating duplicate SPRs. It will provide higher visibility in tracking SPRs using a customizable or ad hoc report capability. Portalization of the SPR database is projected for a production release by mid-summer 2004. ■



Commander's Tactical Terminal

Three Channel (CTT3) Revision F and User's Specific Processor 11A Software and Release Notes Now Available

Submitted by George Lednev and Tejash Maisuria, CECOM SEC

The CTT3 is a three channel ultra high frequency (UHF) Satellite Communications (SATCOM)/ line-of-sight intelligence dissemination terminal. The CTT3 provides the capability to receive three simultaneous channels of intelligence information from the Tactical Reconnaissance Intelligence eXchange System (TRIXS), Tactical Information Broadcast Service (TIBS), Tactical Related APplications (TRAP), and TActical Data Intelligence eXchange System-B (TADIXS-B) network broadcasts. Also, the CTT3 provides the capability to receive two simultaneous channels of TRIXS, TIBS, and TRAP/TADIXS-B while transmitting and receiving TRIXS or TIBS on the third channel.

On behalf of PM Joint Tactical Terminal/Common Integrated Broadcast Service-Modules (JTT/CIBS-M), the CECOM Software Engineering Center (SEC) CTT team completed and began distributing CTT3 Revision F (REV F) and User's Specific Processor (USP) 11A software and Software Release Notes to CTT3 users, Host System Managers (HSMs), and software maintainers.

CTT3 Revision F Software

Revision F corrected the following problems:

- During heavy traffic the communication buffers in the CTT3 could not keep up, causing infrequent loss of TRAP Data Dissemination Service network data.
- USP download was inadvertently allowed while signed on, causing the radio and the host system to lock up until both were powered back up or rebooted to recover, and possibly requiring the USP to be cleared via a Memory Clear operation.
- TIBS bandwidth requests made during or prior to sign-on were delayed until after the TIBS terminal was signed on to the CTT3 Master.
- Error in bandwidth allotment algorithm occasionally prevented CTT3 users from transmitting data over the TIBS network.
- CTT3 users requesting high priority access to the TIBS network to transmit data were not getting the required priority access (e.g., Bandwidth High Priority Rapid Revisit request not granted).
- CTT3 users requesting access to the TIBS network to transmit data, using the bandwidth request message with a 20-second revisit interval, were never given access.
- When the CTT3 designated as the TIBS Network Controller/Master initiated a request to pass network control over to another CTT3 user, the master pass would fail. Therefore, all active network participants would have to sign on to the network again, and transmission of TIBS network data would be delayed.
- The General Purpose Link (GPL) Channel Setup Message was not being processed correctly preventing CTT3 users using the Channel 1 GPL port from transmitting data over the CTT3 GPL.

No Host Tactical Data Processor (TDP) software changes and no particular USP version are required to take advantage of these corrections.

USP 11A Software

USP 11A incorporated new functionality and corrections to previous USP baseline anomalies.

USP 11A gives CTT3 users the ability to receive all the new tactical intelligence data available on the TIBS network as documented in the latest version of the TIBS broadcast specification (Revision F) and the latest version of the Tactical Data Intercomputer Message Formats message output format (also REV F).

USP 11A also corrected the following problems:

- Incorrect Extended Time of Intercept passed to CTT3 users.
- Incorrect fixed duration data related to the reference collector passed to CTT3 users.
- Failure to reset all related Pulse Rate Interval (PRI) fields on receipt of a PRI Reset.
- When a CTT3 user performed a TIBS Query/Text Block, Time Group Request Query, or Time Interval Request Query using illegal/undefined location values and or addressing, the CTT would accept the out of bounds value and return incorrect values.

Continued on page 10

(Continued from page 9)

CTT3 Revision F and USP 11A Software Release Notes

The CTT3 REV F and USP 11A corrections, enhancements, and deletions are described in the SEC-prepared USP 11A and CTT3 Revision F Software Release Notes. Both Software Release Notes provide a description of implementation of the previously existing anomaly or new/removed functionality and provide guidance as to whether CTT3 Revision F (or USP 11A) software installation is required to support the USP 11A (or CTT3 REV F) changes. The release notes help clarify the impacts of the USP (or CTT3 REV F) changes on the CTT3 TDP (e.g., Common Ground Station, Joint Tactical Ground Station, USMC TERPES, etc.) software if USP 11A (or CTT3 REV F) is, or is not, utilized. In addition, possible problems that have been observed to date when using the CTT3 and USP interface are provided, as are some guidelines to aid the HSMs and software maintainers in their determination about whether or not to install USP 11A (or CTT3 REV F), with or without CTT3 REV F (or USP 11A), and with or without requiring a Host TDP software update.

The US Air Force Detachment 2 and Raytheon, Greenville, Texas, the developer and maintainer of the USP software, played an integral part in assisting SEC in preparing the USP 11A software release notes. PM JTT/CIBS-M and the SEC Team (which includes Raytheon System Company, Saint Petersburg, Florida, the developer of the CTT3 software) played an integral part in assisting SEC in preparing the CTT3 REV F software release notes. Feedback on past and present CTT3 and USP Software Release Notes has been extremely positive from Host System Managers/ Maintainers and CTT3 users. ■

Post Production Software Support for the Satellite Configuration Control Element System

Submitted by J. Jamison, CECOM SEC

The Satellite Configuration Control Element (SCCE), AN/FSC-91, provides operational command and control of the Defense Satellite Communications System (DSCS) III satellites to satisfy real-time user requirements. The SCCE is capable of monitoring the real-time downlink telemetry from two DSCS III satellites simultaneously, processing and displaying operator-selected telemetry data for review and journalizing the processed and unprocessed telemetry for subsequent analysis. The SCCE generates commands to reconfigure satellite communications channels and antennas, and provides control of COMSEC (communications security) equipment. The system also provides an alternative means of commanding spacecraft maneuvering and routine housekeeping as backup to the US Air Force Satellite Control Facility. The system is also capable of detecting and locating communications jammers, and reconfiguring the satellites to null the jamming signals.

Currently, SEC representatives have modified the SCCE software and databases for two recently launched DSCS III satellites. For the A3 satellite, which was launched on 10 March 2003, the SEC has provided an engineering baseline of the A3 SCCE database to the Defense Satellite Communications Operations Centers (DSCSOCs) for On-Orbit-Testing (OOT). OOT usually lasts 90 days and changes to the engineering baseline database are delivered to SEC for incorporation into the final database. On completion of the OOT, the SEC will release and field a final A3 database to the DSCSOCs. This database will include any changes that resulted from OOT.

SEC representatives have also modified the SCCE software and database for the B6 satellite. This software and database was provided to the DSCSOCs in June 2003. The B6 satellite software modifications consisted of software changes to accommodate the use of a new battery pack in the B6 satellite. At the time of this writing, the final software and database release for the B6 satellite is scheduled to take place in the November–December 2003 time frame.

SEC also provides new database upgrades to the field three times a year. These databases correct out-of-limit alarms, which are the result of seasonal changes and degradation of the DSCS III satellite due to aging. The SEC released DB71 and DB72 to the DSCSOCs in October 2002 and February 2003, respectively. ■

AN/MLQ-40(V)3 Detecting System Countermeasures (Prophet Block I System) Software Support Transitions to CECOM SEC

Submitted by Jerry Kunert, CECOM SEC

Prophet is a Communication Intelligence system that intercepts, locates, and reports the source of hostile command and control communication transmissions to provide force protection and enhanced situational awareness/situational understanding in direct support of the maneuver brigade. Prophet will be fielded as two functional subsystems: Prophet Collector Vehicle and Prophet Control Vehicle. Prophet operates from a mounted HMMWV (High Mobility Multipurpose Wheeled Vehicle), for stationary and on-the-move capability, with a dismounted manpack configuration. Prophet Block II/III will also have the ability to electronically attack critical communications nodes.

Responsibility for Prophet Block I System Post Deployment Software Support is transitioning from Product Manager Prophet to the CECOM Software Engineering Center. CECOM SEC will provide the infrastructure for both direct on-site and Depot level support for the AN/MLQ-40(V)3 Detecting System Countermeasures (Prophet Block I System). Field Software Engineers (FSEs) assigned to the SEC Intelligence Fusion Systems Tactical Automation Support Branch will provide the direct on-site level support. The FSE and the system users will be supported by Subject Matter Experts at the Depot for problem identification assistance and software problem validation on the Depot test bed. The Depot will be the single focal point for software problem reporting, software problem resolution, software upgrades/ enhancements, software baselines, and distribution of map data. The Depot will provide assistance in converting National Imagery and Mapping Agency map data, Compressed ARC Digitized Raster Graphic or ARC Digitized Raster Graphic format, to the system specific format or will provide the Region of Interest in the converted format on request. The total support infrastructure is projected to be fully operational starting FY04, however, system users can now obtain assistance and or answers to inquiries by contacting the CECOM SEC Prophet Project Leader or by accessing the SIGINT/ Surveillance Global Support Center

https://rdit.army.mil/SIGINT/menu.cfm

bypassing the User Login Option and selecting the Report a Problem/Incident option to complete a Field Incident Report for the Prophet System. ■

Evolving Multi-Service Electronic Warfare Data Distribution System

Submitted by Robert A. Hankins, CECOM SEC

Those of you who have frequented the Multi-Service Electronic Warfare Data Distribution System (MSEWDDS) over the past years have seen a progressive improvement in our website, telephone access, and paperwork.

The website is now more user friendly than it was in the first year of our connection to SIPRNET (Secret Internet Protocol Router Network). The site now contains lists of all libraries available as well as electronic users forms. When you go to the user sign-up area you can fill in the users form and then create your account. The users form is also available on our unclassified information only website, which makes it easer for most people, especially TASO/CAO's (CAO is a Navy term), who must print out their form for signatures before faxing it to us.

STU-III access looks the same as when the system was implemented in April of 1992. This is necessary to reduce the access time it takes for our users who have 2400 baud STU-IIIs and or noisy telephone lines. The menuing system is about as streamlined as it can be. The improvements that we made in STU-III access are in the areas of hardware and the quality of our telephone lines.

New for this year is our users database. This database reduces the need to send in the old memo form and TASO forms. Now you can access the users form by our SIPRNET website in the sign-up area or on our new unclassified informational website, which makes it easier for most to do the paperwork part of establishing an MSEWDDS account. Users fill out the information and just submit the form. TASOs must print the form, sign it at the TASO/CAO location, and have it signed by the appointing official. The form is then faxed to us. Additionally, TASOs must fax us a list of authorized users or send an email to the SYSOP account on the MSEWDDS.

The MSEWDDS help desk is manned by Army and Air Force personnel who are dedicated to serving the soldier.

The unclassified secure website is

https://wwwmil.53wg.eglin.af.mil/milweb/msewdds

MSEWDDS help desk telephone numbers are

DSN: 872-2166

Commercial: (850) 872-2166 ■

New Sun Workstation Software Package Releases for the MSE and TRI-TAC Systems

Submitted by Keith Brenner, CECOM SEC

The SEC developed two new Workstation Software Package (WSP) versions for the Army's Tactical Circuit switches, WSP 2003.5.2 and WSP 2003.8.0. The circuit switches that use the WSP software are the AN/TTC-56 (V) 1 Single Shelter Switch and the Mobile Subscriber Equipment (MSE) switches, which include the AN/TTC-47 Node Center Switch, the AN/TTC-46 Large Extension Node, and the AN/TTC-50 Force Entry Switch. MSE switches that use the WSP software include the Tactical High Speed Data Network and the Asynchronous Transmission Mode First Digitized Corps switches. The primary reason for two new WSP versions is to provide corrections to high priority anomalies reported by the field user and an update of the Solaris operating system. The workstations in the Army's tactical switches currently use Solaris version 2.5.1, which recently went End of Life, meaning the vendor no longer supports it.

SEC and PM WIN-T managed the migration of the WSP functionality to the Solaris version 2.8 operating system (commonly called Solaris 8). This vendor-supported operating system has better security protection, and supports newer versions of other COTS (commercial off-the-shelf) software used by the workstation, such as HP Openview. Both new versions have identical functional upgrades. For example, switch operators will have a chat server and be able to make attachments to email. The Sendmail program has been upgraded to guard against Denial of Service attacks. A software problem was fixed that caused a halt in the transmission of reports to network management systems using the Simple Network Management Protocol.

The new WSP software successfully completed formal testing and received a Full Software release from the CG of CECOM on 1 July 2003. SEC plans to distribute WSP 2003.5.2 (based on Solaris 2.5.1) on CD ROM immediately, then upgrade users to WSP 2003.8.0 (based on Solaris 8) by a round-robin of the removable system disks during the rest of FY03 and early FY04. ■

Support of Operation Iraqi Freedom

Submitted by Keith Brenner, CECOM SEC

SEC deployed a field software engineer in support of the 22nd Sig Bde deployed in SW Asia for Operation Iraqi Freedom. The engineer helped users configure their switches and routers, advised network managers on more efficient setups, assisted the Warfighters in troubleshooting the circuit switches, and collected information on software anomalies (memory dumps and system logs). SEC developed a fix to a slowdown of the flood search process and fielded it as an emergency software release (CSOLOP version RD302195). This version later received full materiel release (1 July 2003) along with workstation software described in the article above.

The 22nd Sig Bde requested four enhancements to the tactical circuit switch software. These enhancements will enable network managers to identify personnel who illegally obtain call precedence, and allow managers to easily regulate which callers have access to other area codes, especially DSN area codes. These measures are designed to reduce traffic so that essential users can make priority calls. Other improvements will provide the switch operators with a way to filter the amount of certain warning messages that have been slowing down the switch workstations, and provide the switch ID of the distant end switch on each inter-switch link to network management systems. SEC has developed software to implement these requests, and is currently testing it. When the software is released, the SEC field software engineer will return to SW Asia to assist the 22nd Sig Bde with installation, training, and use of the new capabilities. ■

ARAT-R^{2}CIL Establishes OCONUS SIPRNET Dial-Up Numbers

Submitted by Mike Crapanzano, ARAT-R^{2}CIL, SRI International

The Electronic Combat Branch Army Reprogramming Analysis Team (ARAT)-Rapid Reprogramming Communication Infrastructure Lab (R^{2}CIL) SIPRNET (Secret Internet Protocol Router Network) communications support team has established toll free dial-up numbers in both South Korea and Germany, to go along with the current CONUS (Continental United States) toll free dial-up number, based on feedback received from the Warfighter community. These numbers have been in use and tested over the past several months, with good feedback received from the Warfighter community.

Overseas dial-up has always been a negative issue because of noisy DSN lines, lack of long distance access, and the need for quality phone lines for a STU-III or STE to go secure. Over the past several months the ARAT-R^{2}CIL staff has seen a dramatic rise in dial-up customer access from South Korea via the new toll free number. All the dial-up user will need is commercial line access to use the numbers in both Korea and Germany.

The ARAT-R^{2}CIL staff is working closely with CECOM SEC's Korean Software Support Representatives (KSSO) and European Software Support Representatives (ESSO). We are also assisting local users on setting up their laptops with the new dial-up software and procedures to adapt very easily to the new toll free number dial-up. For those interested in the new procedures and OCONUS (Outside CONUS) toll free numbers, please contact the CECOM SEC R^{2}CIL staff at 732-532-9395 or DSN 992-9295 or via unclassified email:

ARAT@ems.sed.monmouth.army.mil.

You can also speak to the SEC KSSO and ESSO support contacts in the respective theaters, as follows:

KSSO, Mr. Sok Kim, DSN 315-741-6052

ESSO, Mr. Andrew Poulter, DSN 314-375-8519

As stated, this idea originally generated from the field, so if you know of other areas that would benefit from a toll free dial-up number, please contact R^{2}CIL staff. ■

For Your Information

Now Available on the Web

All 29 previous issues of the "ARAT Bulletin," "A/IEW Bulletin," and "BSSD Bulletin" are now available on the ARAT website. The issues are available in HTML format for on-line viewing, as well as in PDF and MS Word format for viewing and downloading.

Future issues will also be posted on the site. You are encouraged to download any issue (or issues) for local reproduction and distribution within your agency.

The ARAT website can be accessed at http://www.sec.army.mil/arat/ or from a link on the A/IEW website at http://www.sec.army.mil/aiew/.

Help Us Help You

If you are moving, have moved, or your address is listed incorrectly on the mailing envelope, please email Kimberly.Weaver@mail1.monmouth.army.mil (alternate: Sheri.Charpie@mail1.monmouth.army.mil) with the correct address. Many bulletins are returned for incorrect addresses and unknown addressees. We would like to reduce the amount of returned mail and ensure that all of our customers receive the latest issue of the "BSSD Bulletin." Thank you for your support.

ARAT Rapid Reprogramming Communications Infrastructure Laboratory (R^2CIL)

Telephone:

#1 (732) 532-9395, DSN: 992-9395 #2 (732) 532-9392, DSN: 992-9392

Email:

Unclassified: ARAT@ems.sed.monmouth.army.mil

SIPRNET: webmaster@arat.army.smil.mil

ATTENTION ELECTRONIC WARFARE OFFICERS!

Electronic Warfare Officers requiring Memory Loader/Verifier (MLV) reprogramming kits, copies of the "ARAT Software and Documentation Toolbox" CD or the "Mission Data Set Training" CD should contact either

Mr. Mike Crapanzano
(DSN: (312) 992-9392/CML: (732) 532-9392) (michael.crapanzano@mail1.monmouth.army.mil)

or R^2CIL
(DSN: (312) 992-9395/9392/CML: (732) 532-9395/9392) (ARAT@ems.sed.monmouth.army.mil)

or make ToolBox CD requests at

NIPRNET: http://www.sec.army.mil/arat/ARAT/ARAT_information/forms/CD_request/cd_request_form.htm
SIPRNET: http://www.arat.army.smil.mil

or make MLV kit requests at

NIPRNET: http://www.sec.army.mil/arat/ARAT/ARAT_information/forms/MLV_request/mlv_request_form.htm
SIPRNET: http://www.arat.army.smil.mil

Coming Events		
Event/Sponsor	**Location**	**Dates**
AUSA Aviation Symposium & Exhibition	Arlington, VA	5–7 January 2004
EW and IO Asia/Pacific Region Symposium & Exposition	Adelaide	16–17 February 2004
AOC Roma Symposium & Exposition	Rome	16–19 March 2004

The Battlespace System Support Community—Key Points of Contact			
Agency	**Name/email**	**Comm/DSN**	**FAX Number**
Director, Battlespace Systems Support	Mr. M. Leonard Katz myron.katz@mail1.monmouth.army.mil	(732) 532-5848 DSN 992-5848	(732) 532-3538 DSN 992-3538
Deputy Director, Battlespace Systems Support	Mr. Joseph Ingrao joseph.ingrao@mail1.monmouth.army.mil	(732) 532-0065 DSN 992-0065	(732) 532-3538 DSN 992-3538
Chief, A/IEW Division	Mr. William Walker william.walker@mail1.monmouth.army.mil	(732) 532-1737 DSN 992-1737	(732) 532-5238 DSN 992-5238
Chief, COMM Division	Mr. Jeffrey Downing jeffrey.downing@mail1.monmouth.army.mil	(732) 532-5163 DSN 992-5163	(732) 532-3065 DSN 992-3065
Chief, Intelligence Fusion Division	Mr. Medhat Abuhantash medhat.abuhantash@cecomifs.hua.army.mil	(520) 538-6188 DSN 879-6188	(520) 538-7673 DSN 879-7673
Chief (A), Fire Support	Mr. Milton Smith smithmb@fssec.army.mil	(580) 442-2018 DSN 639-2018	(580) 248-8661
ESSO	Mr. Steven Cooper steven.cooper@hq.amceur.army.mil	49-621-487-3708 DSN (314) 375-3708	49-621-487-7635 DSN (314) 375-7635
KSSO	Mr. John Franz franzj@usfk.korea.army.mil	DSN (315) 741-6094	DSN (315) 741-6582
Chief, ARAT-TA (Eglin AFB)	Mr. Christian Gilbert christian.gilbert@eglin.af.mil	(850) 882-8899 DSN 872-8899	(850) 882-9609 (C) 882-4268 (U) DSN 872-9609 (C) 872-4268 (U)
Chief, ARAT-SE & AV/SN Support Branch (Ft. Monmouth)	Mr. Gary Clerie gary.clerie@mail1.monmouth.army.mil	(732) 532-1337 DSN 992-1337	(732) 532-5238 DSN 992-5238

The BSSD Bulletin Staff

Send comments, changes of address, and articles to:
US Army CECOM
Software Engineering Center
ATTN: AMSEL-SE-WS-AI
Ft. Monmouth, NJ 07703
FAX (732) 532-5238
DSN 992-5238

Editor in Chief
Mr. Joseph Ingrao
BSSD

Technical Editor
Mr. John Hakim
Titan, Inc.

Editor
Ms. Christine Stensig
SRI International

For additional information on the articles in this BSSD Bulletin, please contact Mr. Joseph Ingrao at above email address/phone number.